UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/661,690	09/12/2003	David D. Brandt	03AB014B/ALBRP303USB	7383

7590 07/12/2007

Susan M. Donahue
Rockwell Automation, 704-P, IP Department
1201 South 2nd Street
Milwaukee, WI 53204

EXAMINER	
KIM, TAE K	

ART UNIT	PAPER NUMBER
2109	

MAIL DATE	DELIVERY MODE
07/12/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/661,690	BRANDT ET AL.	
	Examiner	Art Unit	
	Tae K. Kim	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 September 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-31* is/are rejected.

7)☒ Claim(s) *1,2,7,17-19 and 29* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *See Continuation Sheet*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Continuation of Attachment(s) 3). Information Disclosure Statement(s) (PTO/SB/08), Paper No(s)/Mail Date :June 25, 2007; Dec. 12, 2006; Aug. 8, 2006; Jan. 13, 2006; Dec. 22, 2005; May 2, 2005; Jan. 21, 2005; Aug. 30, 2004; .

DETAILED ACTION

This response is in regards to this pending application U.S. 10/661690, filed on September 12, 2003, in which claims 1 – 31, where claims 1, 14, 17, 20, 24, 25, and 28 are independent claims, are presented for examination.

Priority

It is noted that this application appears to claim subject matter disclosed in prior Application No. 60/420,006, filed on October 21, 2002. A reference to the prior application must be inserted as the first sentence(s) of the specification of this application or in an application data sheet (37 CFR 1.76), if applicant intends to rely on the filing date of the prior application under 35 U.S.C. 119(e), 120, 121, or 365(c). See 37 CFR 1.78(a). For benefit claims under 35 U.S.C. 120, 121, or 365(c), the reference must include the relationship (i.e., continuation, divisional, or continuation-in-part) of all nonprovisional applications. If the application is a utility or plant application filed under 35 U.S.C. 111(a) on or after November 29, 2000, the specific reference to the prior application must be submitted during the pendency of the application and within the later of four months from the actual filing date of the application or sixteen months from the filing date of the prior application. If the application is a utility or plant application which entered the national stage from an international application filed on or after November 29, 2000, after compliance with 35 U.S.C. 371, the specific reference must be submitted during the pendency of the application and within the later of four months from the date on which the national stage commenced under 35 U.S.C. 371(b) or (f) or

sixteen months from the filing date of the prior application. See 37 CFR 1.78(a)(2)(ii) and (a)(5)(ii). This time period is not extendable and a failure to submit the reference required by 35 U.S.C. 119(e) and/or 120, where applicable, within this time period is considered a waiver of any benefit of such prior application(s) under 35 U.S.C. 119(e), 120, 121 and 365(c). A benefit claim filed after the required time period may be accepted if it is accompanied by a grantable petition to accept an unintentionally delayed benefit claim under 35 U.S.C. 119(e), 120, 121 and 365(c). The petition must be accompanied by (1) the reference required by 35 U.S.C. 120 or 119(e) and 37 CFR 1.78(a)(2) or (a)(5) to the prior application (unless previously submitted), (2) a surcharge under 37 CFR 1.17(t), and (3) a statement that the entire delay between the date the claim was due under 37 CFR 1.78(a)(2) or (a)(5) and the date the claim was filed was unintentional. The Director may require additional information where there is a question whether the delay was unintentional. The petition should be addressed to: Mail Stop Petition, Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

If the reference to the prior application was previously submitted within the time period set forth in 37 CFR 1.78(a), but not in the first sentence(s) of the specification or an application data sheet (ADS) as required by 37 CFR 1.78(a) (e.g., if the reference was submitted in an oath or declaration or the application transmittal letter), and the information concerning the benefit claim was recognized by the Office as shown by its inclusion on the first filing receipt, the petition under 37 CFR 1.78(a) and the surcharge under 37 CFR 1.17(t) are not required. Applicant is still required to submit the reference

in compliance with 37 CFR 1.78(a) by filing an amendment to the first sentence(s) of the specification or an ADS. See MPEP § 201.11.

Claim Objections

Claim 1 is objected to because of the following informalities: improper grammar in line 5; use "and/or." Appropriate correction is required.

Claim 2 is objected to because of the following informalities: improper grammar in line 2, "...to at least one of identify...", spelled requestor incorrectly in line 2. Appropriate correction is required.

Claim 7 is objected to because of the following informalities: improper grammar in line 1, "...further comprising employing..." Appropriate correction is required.

Claim 17 objected to under 37 CFR 1.75(c), as being of improper form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. It is commonly known to one of ordinary skill in the art that communication protocols FPLMTS, GSM protocol, and CDPD protocol are examples of wireless security protocols.

Claim 18 is objected to because of the following informalities: improper grammar in line 1, "...further comprising encapsulating..." Appropriate correction is required.

Claim 19 is objected to because of the following informalities: improper grammar in line 1, "...further comprising utilizing..." Appropriate correction is required.

Claim 29 is objected to because of the following informalities: improper grammar in line 1, "...further comprising monitoring..." Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1 – 6 and 9 – 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. application 2002/0163920 A1 filed by Walker et al. (hereinafter referenced as Walker) in view of U.S. patent 5,604,914 issued to Akiyoshi Kabe (hereinafter referenced as Kabe) on February 18, 1997.

1. Regarding Claims 1 – 3, 6, and 24, Walker discloses a method and apparatus for providing network security that implements security association to transport data among end points of a communication channel where the security association is used to authenticate the requestor and/or sender of that data and provides path information for the data and comprises of a security and a performance parameter (pgs. 4 and 6, paragraphs 0035 and 0051). The data can also be sent as an open-ended message (pg. 6, paragraph 0053). Walker, however, does not specifically use this method and apparatus within the automated factory setting.

Kabe discloses a communication device used to communicate among different automated factory devices that are joined through a local network (col. 1, lines 14-24). The invention also discloses that within a factory automation environment, there is an international standard communication protocol called Manufacturing Automation Protocol (MAP) (col. 1, lines 15-18). The specific protocol used within the factory network is not what is relevant, but the disclosure that a communication protocol is used within the network to harmonize equipment used in the factory that are typically manufactured by different vendors (col. 1, lines 25-27). It would be obvious to one skilled in the art to combine the teachings within Kabe and Walker to increase routing efficiency and security within an automated factory setting. Once the factory network became accessible remotely, it also needed to be protected by the network security measures used outside the automated factory setting.

2. Regarding Claims 4 and 5, Walker, in view of Kabe, discloses all the limitations of Claim 1. Kabe further discloses several types of devices that can be connected to an automated factory network, such as a computer, controller, robot, etc. (col. 1, lines 27-32). Furthermore, Walker establishes a communication channel within a private, VPN, and information network (pg. 4, paragraph 0035) while Kabe discloses a factory network (col. 1, lines 25-30). Kabe or Walker do not specifically disclose the communication assets being comprised of an I/O device, a Human Interface Machine, a network device, an I/I module, a sensor actuator, a network sensor, and a network device or that the communication channel can be established in a public, wireless, control, or instrumentation network.

However, it is commonly known to one of ordinary skill in the art at the application date that many of the devices connected to the factory network will be or be a combination of an I/O device, a Human Interface Machine, an I/O module, a sensor actuator, a network sensor, and a network device. Additionally, It is commonly known that a system that uses a (virtual private network) VPN tunnel (can also use a public network and a wireless network to establish a communication channel. It is also known that a factory network comprises of controllers and various instruments. It is obvious to one skilled in the art that these various devices would be included in a factory automation environment. For each component to communicate with another in a network setting, they need to be connected to a network device and sensor, comprise of an I/O device or I/O module, and be controlled by a Human Interface Machine. Furthermore, any automated robotics comprises of a sensor actuator to control its movements. A VPN tunnel provides additional security within a public network that uses, for example, IP addresses to route destinations. A factory that includes robotics for factory automation uses those instruments within a control environment.

3. Regarding Claims 9 – 16, Walker, in view of Kabe, discloses all the limitations of Claim 1 above. However, it does not specifically disclose that the factory protocol includes at least a time component, message integrity component, digital signature, sequence field to mitigate replaying old packets, pseudo random sequence, encryption field, or dynamic security adjustment field. There is also no specific disclosure of the factory protocol adapting to a Control and Information Protocol (CIP) or an object model that protects configuration of and transport of data between intelligent devices or

associating with a protocol supporting at least one of a Temporal Key Interchange Protocol (TKIP) and a wireless protocol. Walker or Kabe do not specifically disclose of components providing source validation for identification, perform message digest checking for integrity checking, perform check sum tests, provide integrity mechanisms, provide encryption mechanisms, and provide refresh security protocols. Nor do they specifically reference establishing a network trust by an identification, an authentication, an authorization, or a ciphersuite negotiation. Neither is the specific employment of an Elliptical function, an Aziz/Diffie Protocol, a Kerberos protocol, a Beller-Yacobi Protocol, an Extensible authentication protocol (EAP), an MSR+DH protocol, a Future Public Land Mobile Telecommunication Systems Wireless Protocols (FPLMTS), a Beller-Chang-Yacobi Protocol, a Diffie-Hellman Key Exchange, a Parks Protocol, an ASPECT Protocol, a TMN Protocol, RADIUS, Groupe Special Mobile (GSM) protocol, a Cellular Digital Packet Data (CDPD) protocol, a Control and Information Protocol (CIP) network, a DeviceNet network, a ControlNet network, an Ethernet network, DH/DH+ network, a Remote I/O network, a Fieldbus network, a Modbus network, or a Profibus network with the system disclosed in the mentioned references. Walker or Kabe do not disclose the use of a security field to limit access based upon line of sight parameters.

However, it is commonly known to one of ordinary skill in the art at the application date that communication protocols used within factory networks, such as TCP/IP or MAP, are comprised of various combinations of a time component, message integrity component, digital signature, encryption field, sequence fields, pseudo random sequence, and dynamic security adjustment field. It is also commonly known to one of

ordinary skill in the art that various wireless, including those using line of sight parameters, and communication protocols can be used within an automated factory network, such as CIP, TKIP, EAP, Aziz/Diffie Protocol, Kerberos protocol, Beller-Yacobi Protocol, MSR+DH protocol, FPLMTS, Beller-Chang-Yacobi Protocol, Diffie-Hellman Key Exchange, Parks Protocol, ASPECT Protocol, TMN Protocol, RADIUS, GSM protocol, CDPD protocol. Furthermore, these various protocols can be used to establish the following networks: CIP, DeviceNet, ControlNet, Ethernet, DH/DH+, a Remote I/O, Fieldbus, Modbus, and Profibus. It is obvious to one skilled in the art that a method of providing network security, such as the one described in Walker, would be adaptable and implemented on multiple network protocols that existed at that time. It is also obvious to one skilled in the art that a method of providing network security can "tunnel" through multiple types of networks that use such network protocol, such as the ones described above. Furthermore, the use of the various combinations of the aforementioned components for any communication and security protocol ensures proper transmission and authorized access of information across a network. The broad compatibility within networks and protocols available follows within the concept of allowing various components, which are more than likely to be manufactured by different vendors, to communicate seamlessly. Allowing access to the factory network wirelessly, virtually, or remotely improves the accessibility of the network and communications between an authorized user and component or between components.

4. Regarding Claims 17 – 19, Walker discloses a method and apparatus for providing network security that implements security association to transport data among

end points of a communication channel where the security association is used to authenticate the requestor and/or sender of that data and provides path information for the data and comprises of a security and a performance parameter (pgs. 4 and 6, paragraphs 0035 and 0051). Walker, however, does not specifically use this method and apparatus within the automated factory setting or the specific utilization of a Temporal Key Interchange Protocol (TKIP) or an Elliptical function in the wireless security protocol.

Kabe discloses a communication device used to communicate among different automated factory devices that are joined through a local network (col. 1, lines 14-24). The invention also discloses that within a factory automation environment, there is an international standard communication protocol called Manufacturing Automation Protocol (MAP) (col. 1, lines 15-18). The specific protocol used within the factory network is not what is relevant, but the disclosure that a communication protocol is used within the network to harmonize equipment used in the factory that are typically manufactured by different vendors (col. 1, lines 25-27). It would be obvious to one skilled in the art to combine the teachings within Kabe and Walker to increase routing efficiency and security within an automated factory setting. Once the factory network became accessible remotely, it also needed to be protected by the network security measures used outside the automated factory setting. Kabe does not specifically disclose that the communication protocol utilizes TKIP or an Elliptical function in the wireless security protocol.

However, it is commonly known to one of ordinary skill in the art at the application date that communication protocols FPLMTS, GSM protocol, and CDPD protocol are examples of wireless security protocols that are used in various communication networks. It is also known that TKIP has been used to improve wireless security among compatible devices while an Elliptical function provides audio communication. It is obvious to one skilled in the art that a method of providing network security would be adaptable and implemented on multiple network protocols that existed at that time, particularly with the benefits of remote accessibility of wireless communication. The benefits using TKIP and Elliptical functions in the wireless security protocol are increased security and the ability to communicate through sound if desired. Allowing access to the factory network wirelessly, virtually, or remotely improves the accessibility of the network and communications between an authorized user and component or between components and furthers the concept of an automated system.

5. Regarding Claim 20 and 21, Walker discloses a method and apparatus for providing network security that implements security association to transport data among end points of a communication channel where the security association is used to authenticate the requestor and/or sender of that data and provides path information for the data and comprises of a security and a performance parameter (pgs. 4 and 6, paragraphs 0035 and 0051). Walker, however, does not specifically use this method and apparatus with an factory network setting where network security establishes a communications session with an automation asset via a strong security protocol and exchanges data with the automation asset in accordance with real time communications

via a lightweight security protocol that induces minimal impact on a system's performance.

Kabe discloses a communication device used to communicate among different automated factory devices that are joined through a local network (col. 1, lines 14-24). The invention also discloses that within a factory automation environment, there is an international standard communication protocol called Manufacturing Automation Protocol (MAP) (col. 1, lines 15-18). The specific protocol used within the factory network is not what is relevant, but the disclosure that a communication protocol is used within the network to harmonize equipment used in the factory that are typically manufactured by different vendors (col. 1, lines 25-27). It would be obvious to one skilled in the art to combine the teachings within Kabe and Walker to increase routing efficiency and security within an automated factory setting. Once the factory network became accessible remotely, it also needed to be protected by the network security measures used outside the automated factory setting. Kabe does not specifically disclose that the network security establishes a communications session with an automation asset via a strong security protocol and exchanges data with the automation asset in accordance with real time communications via a lightweight security protocol that induces minimal impact on a system's performance.

However, it is commonly known to one of ordinary skill in the art at the application date that several communication protocols use interrupts for higher priority communications. The interrupts in these various communication protocols can skip several layers of the OSI model, decreasing the security level of that communication. It

is also known that these interrupts can be used to dynamically switch between communications with stronger security and lightweight security. It is obvious to one skilled in the art that these interrupts can be used for real-time communication to switch to dynamically from stronger to lighter security protocols. It is also obvious that security protocols are used within various layers of the OSI layers and the more layers associated with such protocols, the more secure it can become. Allowing communications between components using very low-level encryption will minimize the impact on the components' performances and further utilization of the more "complex" OSI layers can strengthen the security protocol.

6. Regarding Claims 22 and 23, Walker, in view of Kabe, discloses all the limitations of Claim 20 above. It does not specifically disclose that the security protocol comprised of various combinations of a time component, message integrity component, digital signature, encryption field, sequence fields, pseudo random sequence, and dynamic security adjustment field or that the path component further comprises of a requestor identifier.

However, it is commonly known to one of ordinary skill in the art at the application date that communication protocols used within factory networks, such as TCP/IP or MAP, are comprised of various combinations of a time component, message integrity component, digital signature, encryption field, sequence fields, pseudo random sequence, and dynamic security adjustment field. It is further known that within the communication protocol, information regarding both the sender and requestor of said information is embedded and used to facilitate the data transfer and to authenticate the

sender and recipient. The use of the various combinations of the aforementioned components for any communication and security protocol ensures proper transmission and authorized access of information across a network.

Claims 7 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Walker, in view of Kabe, as applied to Claim 6 above, and further in view of U.S. application 2003/0014500 A1 filed by Trevor et al. (hereinafter referenced as Trevor).

7. Regarding Claims 7 and 8, Walker, in view of Kabe, discloses all the limitations of Claim 6. It does not, however, disclose that the security system comprises of employing weak encryption protocols for real-time performance and strong security protocols for added security.

Trevor discloses a communication technique where several data processing routines can be implemented in a process control system and be applied to any desired data analysis or data processing routines, including monitoring and real-time optimization routines (pg. 8, paragraph 0051). It is obvious to one skilled in the art that this technique would be implemented in an automated factory network. The implementation of these routines will enable an automated factory to work more efficiently and continuously without human intervention. These routines can determine the necessary security measures needed for all communications within the network using multiple parameters, including real-time performance parameters. One can employ weaker encryption protocols for data necessary for real-time performance and implement stronger security protocols for other data. Furthermore, the monitoring

routines can continuously screen for selected parameters (security and performance) and dynamically change the factory protocol as desired to improve self-sufficiency. Without the use of process routines, the benefits of an automated system will not be fully utilized.

Claims 25 – 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Walker, in view of Kabe, and further in view of "AI Techniques Applied to High Performance Computing Intrusion Detection" by Susan M. Bridges et al. (hereinafter referenced as "Bridges").

8. Regarding Claims 25 – 31, Walker discloses a method and apparatus for providing network security that implements security association to transport data among end points of a communication channel where the security association is used to authenticate the requestor and/or sender of that data and provides path information for the data and comprises of a security and a performance parameter (pgs. 4 and 6, paragraphs 0035 and 0051). Walker, however, does not specifically use this method and apparatus within the automated factory setting or the utilization of an intrusion detection component or methodology.

Kabe discloses a communication device used to communicate among different automated factory devices that are joined through a local network (col. 1, lines 14-24). The invention also discloses that within a factory automation environment, there is an international standard communication protocol called Manufacturing Automation Protocol (MAP) (col. 1, lines 15-18). The specific protocol used within the factory

network is not what is relevant, but the disclosure that a communication protocol is used within the network to harmonize equipment used in the factory that are typically manufactured by different vendors (col. 1, lines 25-27). Kabe, however does not specifically disclose the utilization of an intrusion detection component or methodology.

Bridges discloses a system and method of using artificial intelligence within a high performance computer environment detect intrusions in the network. Specifically, Bridges discloses its use within a cluster computing architecture using both TCP/IP and Giganet networking protocols (pg. 1, paragraph 3). The system combines both anomaly and misuse detection mechanisms and uses both network traffic and system audit date as inputs, meaning the intrusion detection is both host and network-based (pg. 1, paragraph 1). Fuzzy logic is used with association rules and frequent episodes to "learn" normal patters of the system behavior. If certain events leave a set of patterns that are below a specified threshold, the system issues an alarm. The system can also implement rules that match patters of known attacks or patterns that are commonly associated with suspicious behavior to identify attacks (pg. 2, paragraph 5). The system also uses a Decision Module determine the security actions once an attack is detected (pg. 9, paragraph 1). It is obvious to one skilled in the art that an automation security system that will monitor for intrusions and unauthorized access is necessary due to the possibility of address spoofs or tunneling into the network. The Bridges system particularly functions well in an automated system where performance degradation is generally not acceptable. Furthermore, the ability of the Bridges system

to use multiple communication protocols that are also usable in an automated security system makes the Bridges system very desirable as an intrusion detection system.

Additional References

Additional references that are relevant to the pending application and not cited: U.S. 2003/0014500; U.S. 5,539,906; U.S. 2003/0195861; U.S. 6,357,010; U.S. 6,477,651; U.S. 2002/0199122; U.S. 6,647,497; U.S. 2004/0073900; U.S. 2003/0126466; "Manufacturing Automation Protocol (MAP): Review and Analysis," by Michael Kaminski, New Directions in M.I.S. Management: Seminar, Melbourne, FL, Nov. 13-15, 1985.

Contacts

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tae K. Kim, whose telephone number is (571) 270-1979. The examiner can normally be reached on Monday – Friday (8:00 AM – 5:00 PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Frantz Coby, can be reached on (571) 272-4017. The fax phone number for submitting all Official communications is (703) 872-9306. The fax phone number for submitting informal communications such as drafts, proposed amendments, etc., may be faxed directly to the examiner at (571) 270-2979.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at (866) 217-9197 (toll-free).

TKK

July 2, 2007

Frantz Coby

FRANTZ COBY
SUPERVISORY PATENT EXAMINER